MARIE STOPES INTERNATIONAL ETHIOPIA (MSIE)

INFORMATION SYSTEM AND TECHNOLOGY

USERS REGULATION

Addis Ababa

January 2010

Table of Contents

1. INTRODUCTION 1
2. SCOPE 1
3. RESPONSIBILITY 1
4. ACCEPTABLE USE REGULATIONS 2
   4.1 General use and ownership 2
   4.2 Security and proprietary information 2
   4.3 Unacceptable use 3
   4.4 System and network activities 4
      4.4.1 E-mail and communications activities 6
      4.4.2 Web activities 6
5. ANTIVIRUS REGULATIONS 7
   5.1 General guidelines 7
6. E-MAIL REGULATIONS 8
   6.1 General use of the e-mail systems 8
   6.2 Use of encryption 9
   6.3 Restrictions on incoming and outgoing messages 9
   6.4 Handling attachments 10
   6.5 Message forwarding 10
   6.6 Handling alerts on security 10
   6.7 User Data Backup 10
   6.8 Purging electronic messages 11
   6.9 Addendum on outbound electronic mail 11
7. INTERNET REGULATIONS 12
   7.1 General use of the internet 12
   7.2 Respecting intellectual property rights 13
   7.3 Respecting privacy rights 13
   7.4 Use of web based e-mail accounts 14
8. IT EQUIPMENT SECURITY REGULATIONS 14
   8.1 General guidelines 14
9. PASSWORD REGULATIONS 17
   9.1 General password construction guidelines 17
   9.2 Password protection standards 18
10. USE OF LAPTOP COMPUTERS REGULATION 19
11. SOFTWARE INSTALLATION AND USAGE PROCEDURES 20
12. POLICY ENFORCEMENTS 20

1. INTRODUCTION

The purpose of this document is to outline the acceptable use of Marie Stopes International Ethiopia's (MSIE) computer equipment and services so as to protect the organization from illegal or damaging actions by individuals, either knowingly or unknowingly. This document outlines the rules for acceptable use of various systems, such as e-mail, internet, intranet and data systems etc.

Effective security is a team effort involving the participation and support of every user of information systems. It is the responsibility of every user to know these regulations and to conduct activities accordingly. The regulations are in place to protect the user and MSIE. Inappropriate use exposes MSIE to risks, including virus attacks, compromise of network systems or services and possible legal issues.

2. SCOPE

The regulations apply to employees (full-time, part-time, and temporary staff), volunteers, consultants, and other third party persons at MSIE, and cover all equipment being operated on MSIE property or located elsewhere on behalf of MSIE. Internet, intranet and extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing e-mail, web browsing and FTP(File transfer protocol), are covered by these regulations.

3. RESPONSIBILITY

It is the responsibility of all Directors /Managers to ensure that the contents of this document are communicated to all users and observed by them. In turn all users are responsible for complying with the regulations.

4. ACCEPTABLE USE REGULATIONS

4.1 General use and ownership

While MSIE's network administration desires to provide a reasonable level of privacy, users should be aware that data created by users on the organization systems becomes the property of MSIE.

Users are responsible for exercising good judgment regarding the reasonableness of personal use. While personal privacy is respected where practical the confidentiality of personal information stored on any network device belonging to MSIE cannot be assured.

MSIE's ISTS (Information System & Technology Services) Department recommends that any information pertaining to MSIE's official business that users consider sensitive or vulnerable be encrypted. For guidelines on information classification and encrypting e-mail and documents, refer to the ISTS Department. For security and network maintenance purposes, authorized individuals within MSIE will monitor equipment, systems, and network traffic on a continuous basis. MSIE reserves the right to monitor, log and audit networks and systems usage. Under no circumstances may information held by users of a personal or quasi personal nature be encrypted.

4.2 Security and proprietary information

IT systems need to be protected from a variety of threats; this applies to communication equipment, PCs and larger pieces of equipment (servers, networks routers, etc). It is the responsibility of each PC user to take all reasonable precautions to safeguard the security of the computer and the information contained within it. This includes protecting it from physical hazards, including spilling liquids; not allowing unauthorised users access to the machine and only using approved software. MSIE will provide mechanisms for ensuring that only authorised users can gain access to computer systems, with

defined user identification and password schemes (refer to Password Regulations). Users must also take care with physical sitting and security of computer equipment and peripherals (refer to IT Equipment Security Regulations).

Users must keep passwords secure and not share accounts. Authorized users are responsible for the security of their passwords and accounts (refer to the Password Regulations).

Users should give to ISTS staff any personal CD,DVD, Floppy Disk,Flash or other data storage media for checking of viruses before using on MSIE computer/ network infrastructure to avoid infection with virus.

All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at ten minutes or less, or by logging off (control-alt-delete for Win2K/XP users) when the host is unattended.
Use encryption of information in compliance with the organization's Encryption Regulations. Because information contained on portable computers such as laptops are vulnerable, users are obliged to take special care.

MSIE will ensure that all hosts used by the user that are connected to the organization's Internet/Intranet, whether owned by the user or MSIE, shall continually execute approved virus-scanning software with current virus definitions, unless overridden by departmental or group regulations (refer to the Antivirus Regulations).

4.3 Unacceptable use

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is a user of MSIE computer equipment or services authorized to engage in any activity that is illegal under local, or international law or that is unacceptably at

variance with MSIE's value expectations for users, while using MSIE-owned resources. Users should not interfere with or disrupt other network users' network services or network equipment. Disruptions include, but are not limited to, propagation of computer worms or viruses, and using the network to make unauthorized entry into any other machines accessible via the network.

The following lists are not exhaustive, and provide a framework for activities that fall into the category of unacceptable use.

4.4 System and network activities

The following activities are strictly prohibited, with no exceptions:

- Violating the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by MSIE

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources; copyrighted music and the installation of any copyrighted software for which MSIE or the end user does not have an active license

- Exporting software, technical information, or encryption software or technology, in violation of international or regional export control laws. Where there is a valid reason for doing so, where there is no perceived legal infringement the authority of a manager senior in grade to the user must be secured.

- Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs) by installing programs , accessing un necessary web sites or bringing those programs with external storage medial (like flash disk) and used in MSIE network.

- A user revealing his/ her account password to others or allowing the use of his / her account

- Using a MSIE computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or workplace laws in the user's local jurisdiction

- Making fraudulent offers of products, items, or services originating from any MSIE user account

- Effecting security breaches or disruptions of network communication (Security breaches include, but are not limited to, accessing data of which the User is not an intended recipient or logging in to a server or account that the User is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, Denial of Service, and forged routing information for malicious purposes.)

- Port scanning or security scanning unless prior notification to MSIE's ISTS Department is made

- Executing any form of network monitoring that will intercept data not intended for the User's host, unless this activity is part of the User's normal job or duty(for IT Professionals)

- Circumventing user authentication or security of any host, network, or account. This includes any additional access points such as modems etc without explicit permission from the ISTS Department.

- For security reason, connecting to internet using dial up connection in MSIE LAN (at support Office only) having broadband internet connection is strictly forbidden.

- Interfering with or denying service to any user other than the User's host (e.g., Denial of Service attack)

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session via any means locally or via the Internet/Intranet/Extranet.

- Providing any corporate confidential ,software or sensitive information to unauthorized third parties

4.4.1 E-mail and communications activities

- Sending unsolicited e-mail messages, including junk mail or other marketing material, to individuals who did not specifically request such material (e-mail spam)

- Any form of harassment via e-mail, whether through language, frequencies or size of messages

- Unauthorized use or forging of e-mail header information

- Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies

- Creating or forwarding chain letters or other pyramid schemes of any type

- Transmission or use of unsolicited e-mail originating from within MSIE's networks of non work related material

- Posting non-business-related messages to large numbers of newsgroups (newsgroup spam)

- The e-mail system must not be used for personal political advocacy efforts, religious efforts, private business activities or personal amusement and entertainment (refer to E-mail Regulations).

4.4.2 Web activities

- The user must not visit, download, save or propagate material that contains obscene/pornographic/ music/ program files (*.EXE)/ or other

objectionable material (this list is not exhaustive) nor originate or post such materials. Refer to the Internet Regulations.

- The user must not upload, post, distribute, transmit or disseminate objectionable information, including, but not limited to, any transmissions constituting or encouraging conduct that would constitute a criminal offence, software or content piracy, copyright infringement, give rise to civil liability or otherwise violate any international, or local law, order or regulation. This shall also include any content that victimises, harasses, degrades, or intimidates an individual or group of individuals on the basis of gender, race, religion, sexual orientation, age, disability or ethnicity.

5. ANTIVIRUS REGULATIONS

5.1 General guidelines

Users must use recommended processes to prevent virus problems and must:

- Always run the corporate standard supported antivirus software available from the ISTS Department.
- Ensure that their virus definition is current and up to date.
- Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Users must delete these attachments immediately, and then delete from the “Deleted Items” folder.
- Never download files from unknown or suspicious sources, including from the Internet.
- Avoid direct disk sharing with read/write access to it, unless there is absolutely a business requirement to do so.

- Always scan a floppy diskette/ flash disk or any other data storage media from an unknown source for viruses prior to using it or get advice from ISTS department before using in MSIE systems/network

- Ensure that a current backup of critical data is performed on a regular basis.

- If your PC has intercepted a virus, or if in doubt, contact the ISTS department.

New viruses are discovered almost every day. If your PC is not being updated automatically by the corporate antivirus server specially for branch offices and centers, you will need to follow manual antivirus installation procedures. Where you cannot update the definitions manually, contact the ISTS department immediately to resolve the problem.

6. E-MAIL REGULATIONS

6.1 General use of the e-mail systems

As a productivity and workflow tool, MSIE encourages the use of e-mail for business and work purposes only. The e-mail systems must not be used for personal political advocacy efforts, religious efforts, private business activities or personal amusement and entertainment.

The following activities are strictly prohibited:-

- Creating or forwarding chain letter or pyramid schemes of any type

- Unauthorised use or forging of e-mail header information

- Disclosure of information which includes, but is not limited to, financial information, strategies, plans and products therein, customer or supplier information and computer/network access codes

- Misrepresenting, obscuring, suppressing, or replacing another user's identity on e-mail systems. At a minimum, all computer users must provide their name, and contact details (phone number and signature) in all electronic communications

- The e-mail system should not to be used for the exercise of a user's right to free speech or for political, sexual, ethnic, racial or offensive intentions.

- Users must not upload, post, distribute, transmit or disseminate objectionable information, including, but not limited to actions that would constitute a criminal offence software, content piracy, copyright infringement, give rise to civil liability, violate any international, federal or local law, order or regulation or offends MSIE's value expectations for users. This shall also include any content that victimises, harasses, degrades, or intimidates an individual or group of individuals on the basis of gender, race, religion, sexual orientation, age, disability or ethnicity.

6.2 Use of encryption

Employees are reminded that MSIE e-mail systems do not have a unique encryption mechanism. Therefore, where there is a need to transport/transfer sensitive information pertaining to MSIE's business due care (a need for encryption or alternative media used) should be taken into account by the user or if in doubt contact the ISTS department.

6.3 Restrictions on incoming and outgoing messages

The firewall will be configured in support office network in a manner that will restrict and quarantine offensive material (attachment's to e-mails, subject matter of the e-mail, e-mail body content that contains terms and phrases such as hardcore etc and or pictures or any graphics that contain semi, partial and full nudity etc) on incoming and/or outgoing messages. However, due to the nature of the Organisation's operations certain material cannot be blocked.

6.4 Handling attachments

When sending an attachment to a third party, users must attempt to compress and zip files whenever possible. There is a 1MB attachment restriction limit on sent mail. If you wish to send a file larger than this, contact the ISTS Department. Ensure attachments are scanned with an authorised virus detection software package before opening or execution. In some cases, attachments must be decrypted or decompressed before a virus scan takes place.

6.5 Message forwarding

Users must exercise caution when forwarding messages. MSIE sensitive information should not be forwarded to any party outside MSIE without formal approval from the Country Director/Program Director/Operation Director/Technical Services Director to the user.

6.6 Handling alerts on security

All information security alerts, warnings, viruses are to be reported to the ISTS Department. Where offensive or unsolicited material is received from outside sources, this must not be forwarded or redistributed to either internal or external parties. However the offending e-mail must be forwarded to quarantinespam@mariestopes.org.et where its sender will be added to the corporate spam filter list.

6.7 User Data Backup

All electronic mail messages that contain information relevant to the completion of a business/work related transaction or potentially important reference information, or which have value as evidence of management decision, must be retained for future reference. It is the responsibility of the users to take back up copy of their important data that are not placed on MSIE Servers using appropriate medial like CD,DVD etc and can contact ISTS staff for any assistant they need in doing user data backup.

6.8 Purging electronic messages

Messages that are no longer needed for business purposes must be periodically deleted by users from their 'Inbox' and 'Sent' boxes. It is the responsibility of each user to delete, archive and retain electronic messages.

6.9 Addendum on outbound electronic mail

Footer must be automatically appended to all outbound electronic mail originating from MSIE computers as follows:

Name
Position
Marie Stopes International Ethiopia(MSIE)
Telephone
Email Address
"*The views expressed in this correspondence are those of the author and not necessarily those of Marie Stopes International Ethiopia*"

7. INTERNET REGULATIONS

7.1 General use of the internet

Internet access is a limited, expensive and shared operational resource. As such, this resource, and the use of this resource, needs to be protected and managed. The corporate firewall will provide a certain level of protection and management of internet usage. However, management and user support is equally critical in ensuring a prudent and acceptable usage of this resource.

Internet resource is a productivity and workflow tool, and MSIE encourages the use of Internet for MSIE business and work purposes only obtaining information over the Internet must be restricted to material that is clearly related to MSIE as an NGO organisation.

Incidental personal use is permissible as long as it does not consume more than a trivial amount of resources. Anything more than incidental personal use is permissible on a case by case basis and has to be approved by a manager senior in grade to the user.

The following activities are strictly prohibited on the Internet:-

- Must not upload, post, distribute, transmit or disseminate objectionable information, including, but not limited to any transmissions constituting or encouraging conduct that would constitute a criminal offence software or content piracy, copyright infringement, give rise to civil liability or otherwise violate any international, federal or local law, order or regulation, or where such action is at variance with MSIE's value expectations for users. This shall also include any content that victimises, harasses, degrades, or intimidates an individual or group of individuals on the basis of gender, race, religion, sexual orientation, age, disability or ethnicity.

- Must not visit, download, create, save or propagate material that contains obscene/pornographic/music/program files/or other objectionable material (this list is not exhaustive).

- Must not use the Internet for any illegal purposes such as making or posting indecent remarks or proposals.

- Must not be used for personal political advocacy efforts, religious efforts, private business activities or personal amusement and entertainment.

7.2 Respecting intellectual property rights

Although Internet Technologies are informal communications, the Copyrights, Design and Patents Act 1988, Computer Misuse Act 1990, and EU Data Protection Directive 1995 will apply. Employees using MSIE Internet systems must not reproduce material unless formal permission has been obtained from the relevant copyright source.

7.3 Respecting privacy rights

MSIE is responsible for operating, maintaining and protecting its Internet infrastructure. Consequently, at its discretion will intercept, disclose, and assist in intercepting or disclosing, electronic data by employing content monitoring systems, message logging systems, and other electronic system management tools. MSIE insists on monitoring and logging all network traffic usage for example Internet sites visited, downloads made, etc

Country management team and other authorized personnel have the right to access any material in users email or on computer at any time. Users should not consider electronic communication, storage or access to be private if it is created or stored at work and users should not store non-work related data like music, pictures, software, etc in the organization network.

7.4 Use of web based e-mail accounts

OWA (Outlook Web Access) is the organisation's standard web based e-mail system. Users to this system can access their corporate e-mails by logging on to http://mail.mariestopes.org.et/exchange and this is particularly important for MSIE remote users (branch office managers and canter coordinators).

8. IT EQUIPMENT SECURITY REGULATIONS

8.1 General guidelines

The physical location of the computer and related equipments needs to be planned with due regard to security considerations and environmental hazards. Potential risks from fire, theft, flooding etc need to be assessed and guarded against. The analysis of physical security should not be confined to the accommodation provided for the servers, but should also consider potential hazards arising from neighbouring accommodation. The physical environment must be maintained in conditions which continue to satisfy standards of physical security and not allow deterioration to occur.

The protection and the efficiency of computers and related equipment is dependent upon the physical and environmental conditions in which these systems operate, reside, function and the mobility of these systems.

There are also a number of hazards (e.g. fire, floods, electricity outage) which are beyond the scope of the systems themselves, and therefore there is a need for good practice to provide overall security for these systems.

It should also be remembered that these physical security and environmental conditions apply not just to the system themselves, but to the surrounding environment, including the storage of documentation and backup devices.

Overall protection of the latter is enhanced if copies of the material are stored off site.

Sensitive IT areas need to be protected by restricting access. Procedures should be in place to control the access of external personnel (eg maintenance engineers) to the sensitive areas where the computers and related equipment are stored.

It is the responsibility of each PC user to take all reasonable precautions to safeguard the security of the computer and or laptop or both. This includes protecting these from physical hazards, such as spilling liquids etc.

- The physical conditions include the structure of the server room, sitting of the servers(s) and related equipment, communications cabinet/switches, air-condition units, UPS etc.
- The environmental conditions include the humidity, temperature and safety of the server room where the computer and related equipment is housed.
- Servers, routers, , network cables and UPS should be housed in a secure area (locked room, cabinets etc).At a minimum, the servers should be housed on a raised platform (ideally with no water pipes in that room) to reduce the risk of flooding.
- At a minimum, for safety, a fire alarm, and or smoke detector and a fire extinguisher should be installed in the server room or the area where the server and backup devices is residing.
- Access to sensitive IT areas (where the servers and backup devices are physically located) should be restricted to authorized IT personnel only. Where access is to be granted to non IT personnel, (engineers etc) formal procedures should be in place. When this access have been authorised and granted, it should be logged and monitored.

- For mobility of the computers and related equipment, sufficient care and packaging should be taken when computers and related equipments are moved from one location to another. When in transit, ensure the laptop(s) are packed tightly with other luggage's to ensure the risk of physical damage is at a minimum. When travelling by air, laptops should be carried as hand luggage at all times.
- Laptops, desktops and servers are susceptible to damage by dust, dirt and interference with electrical circuits. Where possible, a **dust-cover** should be used to ensure the laptops and desktops are free from dust, when not in use.When cleaning, a soft dust cloth should be used.
- As unstable power supply is often delivered by generators and local electricity boards, computers and backup devices should always be connected to an approved surge protector to be protected. Where a laptop/desktop is not allocated to any one user, the department is fully responsible for the care and use of the computer(s) while in their possession.
- Eating or drinking is prohibited in the sensitive IT areas (where physical computers reside) or near the workstations.

Cables (network, etc) connecting computer and related equipment, should never be cut, disconnected, removed or replaced without the prior permission of IT personnel.

Special consideration should be given to the protection of portable computers, as these are more open to theft and physical damage (eg being dropped). Furthermore, the storage of sensitive information on the hard disk of a portable computer should be limited in order to limit the exposure to MSIE in the event of a machine being stolen.

All software applications on the computer(s) must have a valid licence in place for its use.

All IT incidents/issues should be notified by the user to the ISTS department and these will be logged, monitored, escalated and resolved.

9. PASSWORD REGULATIONS

The following guidelines will apply:

- All system-level passwords (e.g NT admin, application administration accounts) must be changed at least on a quarterly basis.
- All production system-level passwords must be part of the ISTS Department administered global password-management database.
- All user-level passwords (e.g., e-mail, Web, desktop computer) must be changed at least every six months. The recommended change interval is every four months.
- Passwords must not be inserted into e-mail messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described in the following sections.

9.1 General password construction guidelines

Passwords are used for various purposes at MSIE. Some of the more common uses include user-level accounts, web based accounts, e-mail accounts, screen-saver protection, voice-mail and local router logins. Everyone should be aware of how to select strong passwords.

Weak passwords have the following characteristics:

- Contain fewer than eight characters.
- Could be found in a dictionary (English or foreign).
- common-use words such as names of family, pets, friends, co-workers, fantasy characters, computer terms and names,

commands, sites, name of a company, hardware, software, words such as "MSIE," "charity", "password" or any derivation thereof, birthdays and other personal information such as addresses and phone numbers, word or number patterns like aaabbb, qwerty, zyxwvuts. 123321, and so on, or any of the above spelt in a reverse order

- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper-, and lower-case characters (e.g., a—a, A—Z)
- Contain digits and punctuation characters as well as letters (e.g.,0—9, !@#$%A8CQ_+I-=" U [1 :";'o?,./,
- Are at least eight alphanumeric characters long
- Are not a word in any language, slang, dialect, jargon, and so on
- Are not based on personal information, names of family, and so on
- Are never written down or stored online.

Users must create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmBIw2R!" or "TmblW>r—" or some other variation. Note: **Do not use** either of these examples as passwords!

9.2 Password protection standards

Do not use the same password for MSIE accounts as for other non-MSIE access (e.g., personal ISP account). Where possible, do not use the same password for various access needs.

Do not share MSIE passwords with anyone, including administrative assistants

or secretaries. All passwords are to be treated as sensitive, confidential MSIE information. Here is a list of "don'ts":

- Don't reveal a password over the phone to anyone
- Don't reveal a password in an e-mail message
- Don't reveal a password to a person more senior in grade
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to coworkers when you go on vacation

Do not use the "remember password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger, etc.). Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on any computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords, which must be changed quarterly). The recommended change interval is every four months. If an account or password is suspected of having been compromised, report the incident to the ISTS Department immediately.

10. USE OF LAPTOP COMPUTERS REGULATION

- Laptop computers should be shared with in department
- Laptop computers should not be used for any personal purpose and should not be used in any other ICT infrastructure out side MSIE's network infrastructure.
- Laptop computers should be left in office when user going on leave.

- Users are responsible for any damage or loss or inappropriate use of laptop computers.

11. SOFTWARE INSTALLATION AND USAGE PROCEDURES

Installing unauthorized software on a computer system, workstation, or network server within MSIE can lead to potential system failures, system degradation or viruses. Hence, only MSIE ISTS team member/System administrators can install software on MSIE computers.

Shareware or Freeware Software is one of the more likely methods by which a system might become infected by a computer virus. Therefore, any download, transfer or installation of Shareware or Freeware Software requires authorization from ISTS.

The acquired software shall be stored securely and carefully managed. It is the responsibility of each end-user to help the designated IT personnel/System Administrator delegated by ISTS to maintain records of all software licenses obtained by MSIE and in use at the organization or work location. Unauthorized software must not be installed, loaded, or used on MSIE computer systems or on personal computers used to conduct MSIE business. Users should avoid practices that are wasteful of storage or processing capacity.

The installed software is used according to the implementation plan guideline and the user manual of the software.

12. POLICY ENFORCEMENTS

An employee who deliberately violates these regulations may be subject to disciplinary action, up to and including termination of employment (refer to Human Resources Policy manual).

Non-staff offenders will be subject to appropriate management action up to and including removal of systems access and termination of contract / service.

I. **Complaints of Alleged Violations:** An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint. The individual is also encouraged to report the alleged violation to the manager overseeing the work unit in which the employee is assigned or to the ISTS, which must investigate the allegation and report to the country management team.

II. **Reporting Observed Violations:** An individual who has direct or indirect knowledge of a violation of this Policy, but has not been harmed by the alleged violation, is duty bound to report the alleged to the manager of the work unit or to the ISTS.

III. **Disciplinary Action:** Alleged violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures for staff as outlined in the Personnel Policy (Human Resource Development Policy and Procedures manual) or any other applicable organization documents or laws. The organization ISTS team members are authorized to investigate alleged violations in the IT system and report findings to the Director of Operation.

IV. **Penalties:** Staff found to have violated this Policy may be subject to penalties provided for in the organization HR policy and Current manuals dealing with the underlying conduct. Violators may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT related access. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with ISTS.

V. **Policy Review:** This Policy may be periodically reviewed and modified upon recommendations of the ISTS or country management team of the organization. Appropriate consultations and discussion will be held on the proposed recommendations before reviewing the Policy and get approval of the country management team